

CheatSheet con 400 comandos para GNU/Linux que deberías saber

By [Leo Romero](#) [@ 4 May 2013](#) [@ 18:42](#) [29 CheatSheet, GNU/Linux, Hack, Tips, Linux OS, Tips, Trucos](#)



Índice:

1. Información del Sistema
2. Apagar (Reiniciar o Cerrar Sesión)
3. Archivos y Directorios
4. Encontrar archivos
5. Montando un sistema de ficheros
6. Espacio de Disco
7. Usuarios y Grupos
8. Permisos en Ficheros (Usa "+" para colocar permisos y "-" para eliminar)
9. Archivos especiales en Debian (Usa "+" para colocar permisos y "-" para eliminar)
10. Archivos y Ficheros comprimidos
11. Paquetes RPM (Red Hat, Fedora y similares)
12. Actualizarse de paquetes YUM (Red Hat, Fedora y similares)
13. Paquetes Deb (Debian, Ubuntu y derivados)
14. Actualizarse de paquetes APT (Debian, Ubuntu y derivados)
15. Ver el contenido de un fichero
16. Manipulación de texto
17. Establecer carácter y conversión de ficheros
18. Análisis del sistema de ficheros
19. Formatear un sistema de ficheros
20. Trabajo con la SWAP
21. Salvo (Backup)
22. CD-ROM
23. Trabajo con la RED (LAN y Wi-Fi)
24. Redes de Microsoft Windows (SAMBA)
25. Tablas IP (PORTAFUROS)
26. Monitorizado y depurando
27. Otros comandos útiles

Información del sistema

1. `arch` -mostrar la arquitectura de la máquina (1).
2. `uname -m` -mostrar la arquitectura de la máquina (2).
3. `uname -r` -mostrar la versión del kernel usado.
4. `dmidecode -q` -mostrar los componentes (hardware) del sistema.
5. `hdparm -I /dev/sda` -mostrar las características de un disco duro.
6. `hdparm -t /dev/sda` -realizar prueba de lectura en un disco duro.
7. `cat /proc/cpuinfo` -mostrar información de la CPU.

🔖 Etiquetas Posts



Las 28 herramientas de hacking más populares del 2013
De un ranking realizado por [Exploit](#) - una comunidad de hackers y expertos en ciberseguridad pagados por [mossack.com](#) durante el 2012. Se

[ver más](#) (17/05/13)



Hackeando un Banco 3 ("Hackear" 14.000+ Tarjetas de Crédito (Gordig))

Después de haber leído la primera edición de esta serie llamada "Hackeando un Banco" (Gordig) y la segunda llamada "Hackeando un Banco 2" (Gordig) he

[ver más](#) (17/05/13)



Crack MD5, SHA1, MySQL, NTLM Free Online

Este script permite a los usuarios de Internet probar los hashes de los contraseñas gratuitos y obtenerlos de forma automática. Funciona

[ver más](#) (17/05/13)



Las 28 herramientas de hacking más populares del 2013

De un ranking realizado por [Exploit](#) - una comunidad de hackers y expertos en ciberseguridad pagados por [mossack.com](#) durante el 2012. Se

[ver más](#) (17/05/13)

Blog archive

[► 2023 \(0\)](#)

[► 2022 \(1\)](#)

[► 2021 \(2\)](#)

[► 2020 \(0\)](#)

[► 2019 \(0\)](#)

[► 2018 \(0\)](#)

[► 2017 \(0\)](#)

[► 2016 \(0\)](#)

[► 2015 \(1\)](#)

[► 2014 \(0\)](#)

[► 2013 \(0\)](#)

[► 2012 \(0\)](#)

[► 2011 \(0\)](#)

[► 2010 \(0\)](#)

[► 2009 \(0\)](#)

[► 2008 \(0\)](#)

[► 2007 \(0\)](#)

[► 2006 \(0\)](#)

[► 2005 \(0\)](#)
CheatSheet con 400 comandos para GNU/Linux que deberías saber.

[► 2004 \(0\)](#)

[► 2003 \(0\)](#)

[► 2002 \(0\)](#)

8. cat /proc/interrupts: mostrar las interrupciones.
9. cat /proc/meminfo: verificar el uso de memoria.
10. cat /proc/swaps: mostrar ficheros swap.
11. cat /proc/version: mostrar la versión del kernel.
12. cat /proc/net/dev: mostrar adaptadores de red y estadísticas.
13. cat /proc/mounts: mostrar el sistema de ficheros montado.
14. lspci -v: mostrar los dispositivos PCI.
15. lsusb -v: mostrar los dispositivos USB.
16. date: mostrar la fecha del sistema.
17. cal 2011: mostrar el almanaque de 2011.
18. cal 07 2011: mostrar el almanaque para el mes julio de 2011.
19. date 041217062011.00: trócar (declarar, ajustar) fecha y hora.
20. clock -w: guardar los cambios de fecha en la BIOS.

Apagar (Reiniciar Sistema o Cerrar Sesión)

1. shutdown -h now: apagar el sistema (1).
2. init 0: apagar el sistema (2).
3. telinit 0: apagar el sistema (3).
4. halt: apagar el sistema (4).
5. shutdown -h hour:minutes.4: apagado planificado del sistema.
6. shutdown -c: cancelar un apagado planificado del sistema.
7. shutdown -r now: reiniciar (1).
8. reboot: reiniciar (2).
9. login: cerrar sesión.

Archivos y Directorios

1. cd /home: entrar en el directorio "home".
2. cd ..: retroceder un nivel.
3. cd ../..: retroceder 2 niveles.
4. cd /: ir al directorio raíz.
5. cd /usr/bin: ir al directorio usr/bin.
6. cd - (previous): ir al directorio anterior.
7. pwd: mostrar el camino del directorio de trabajo.
8. ls: ver los ficheros de un directorio.
9. ls -l: ver los ficheros de un directorio.
10. ls -l: mostrar los detalles de ficheros y carpetas de un directorio.
11. ls -a: mostrar los ficheros ocultos.
12. ls "[0-9]*": mostrar los ficheros y carpetas que contienen números.
13. ls -la: mostrar los ficheros y carpetas en forma de árbol comentando por la raíz (1).
14. ls -lar: mostrar los ficheros y carpetas en forma de árbol, comenzando por la raíz (2).
15. mkdir dir1: crear una carpeta o directorio con nombre dir1.
16. mkdir dir1 dir2: crear dos carpetas o directorios simultáneamente. (Crear dos directorios a la vez)
17. mkdir -p /tmp/dir1/dir2: crear un árbol de directorios.
18. rm -f file: borrar el fichero llamado file.
19. rmdir dir: borrar la carpeta llamada dir.
20. rm -rf dir: eliminar una carpeta llamada dir con su contenido de forma recursiva. (Si lo hace recursivo estoy diciendo que es con su contenido)
21. rm -rf dir1 dir2: borrar dos carpetas (directorios) con su contenido de forma recursiva.
22. mv dir1 new_dir: renombrar o mover un fichero o carpeta (directorio).
23. cp file1: copiar un fichero.
24. cp file1 file2: copiar dos ficheros al mismo.
25. cp dir /: copiar todos los ficheros de un directorio dentro del directorio de trabajo actual.
26. cp -a /tmp/dir1 /: copiar un directorio dentro del directorio actual de trabajo.
27. cp -a dir1: copiar un directorio.
28. cp -a dir1 dir2: copiar dos directorios al mismo.
29. ln -s file1 link1: crear un enlace simbólico al fichero o directorio.
30. ln file1 link1: crear un enlace físico al fichero o directorio.
31. touch -t 0712200000 file1: modificar el tiempo real (tiempo de creación) de un fichero o directorio.
32. file file1: salida (volcado en pantalla) del tipo mime de un fichero texto.
33. lsenc 1: lista de cifrados conocidos.
34. deare -f fromEncoding -c toEncoding inputFile > outputFile: crea una nueva forma del fichero de entrada asumiendo que está codificado en fromEncoding y convirtiéndolo a toEncoding.
35. find . -name "*.jpg" -print -exec convert "{}" -resize 80x60 "0ximage[]" & \; agrupar ficheros redimensionados en el directorio actual y enviarlos a directorios en vista de miniaturas (requiere convert y ImageMagick).

Encontrar archivos

0 - 100000

001/001

002/002

003/003

004/004

Posts from @0blackp0int



Nothing to see here - yet

When they post, their posts will show up here.

View on X

0 - 100000

001/001

002/002

003/003

004/004

005/005

006/006

1. `find / -name file1`: buscar ficheros y directorio a partir de la raíz del sistema.
2. `find / -user user1`: buscar ficheros y directorios pertenecientes al usuario "user1".
3. `find /home/user1 -name "*.bin"`: buscar ficheros con extensión ".bin" dentro del directorio "/home/user1".
4. `find /usr/bin -type f -mtime +100`: buscar ficheros binarios no usados en los últimos 100 días.
5. `find /usr/bin -type f -mtime -10`: buscar ficheros creados o cambiados dentro de los últimos 10 días.
6. `find / -name "*.rpm" -exec chmod 755 {} \;`: buscar ficheros con extensión ".rpm" y modificar permisos.
7. `find / -dev -name "*.rpm"`: buscar ficheros con extensión ".rpm" ignorando los dispositivos genéricos como `cdrom`, `pci-drive`, etc...
8. `locate /tmp`: muestra ficheros con extensión ".ps" ejecutados previamente con el comando "locate".
9. `whereis hola`: mostrar la ubicación de un fichero binario, de ayuda o fuente. En este caso pregunta dónde está el comando "hola".
10. `which hola`: mostrar la senda completa del comando completo o su ubicación ejecutable.

Montando un sistema de ficheros

1. `mount /dev/hda2 /mnt/hda2`: montar un disco llamado hda2. Verifica primero la existencia del directorio "/mnt/hda2"; si no está, debes crearlo.
2. `umount /dev/hda2`: desmontar un disco llamado hda2. Salir automáticamente al punto 1 montada2.
3. `fsck -lan /mnt/hda2`: formatear el dispositivo cuando el dispositivo está ocupado.
4. `mount -n /mnt/hda2 /mnt/hda2`: montar el dispositivo para leer el fichero `/etc/mtab`. Obviamente el fichero es de solo lectura y el disco debe estar `fsck`.
5. `mount /dev/hda /mnt/floppy`: montar un disco flexible (floppy).
6. `mount /dev/cdrom /mnt/cdrom`: montar un cdrom (`/dev/cdrom`).
7. `mount /dev/hda /mnt/cdrecorder`: montar un cd grabable o un `cdrom`.
8. `mount /dev/hda /mnt/cdrecorder`: montar un cd grabable (`/dev/cdrom`) (o `cd-rw`).
9. `mount -o loop file.iso /mnt/cdrom`: montar un fichero o una imagen iso.
10. `mount -t vfat /dev/hda5 /mnt/hda5`: montar un sistema de ficheros FAT32.
11. `mount /dev/dsk /mnt/usbdrive`: montar un usb pen-drive o una memoria (se especifica el tipo de sistema de ficheros).

Espacio de Disco

1. `df -h`: mostrar una lista de las particiones montadas.
2. `ls -lR /usr`: mostrar el tamaño de los ficheros y directorios ordenados por tamaño.
3. `du -sh dir1`: Estimar el espacio usado por el directorio "dir1".
4. `du -sh * | sort -nr`: mostrar el tamaño de los ficheros y directorios ordenados por tamaño.
5. `rpm -q -a -g "%{GID}(%{NAME})" | sort -nr,ln`: mostrar el espacio usado por los paquetes rpm agrupados organizados por tamaño (Nombre, Modulo y otros).
6. `dpkg-query -W -f='${Installed-Size}(%{Package})' | sort -nr,ln`: mostrar el espacio usado por los paquetes instalados, organizados por tamaño (Nombre, Debian y otros).

Usuarios y Grupos

1. `groupadd nombre_del_grupo`: crear un nuevo grupo.
2. `groupdel nombre_del_grupo`: borrar un grupo.
3. `groupmod -n nuevo_nombre_del_grupo viejo_nombre_del_grupo`: renombrar un grupo.
4. `useradd -s "/bin/bash" -g admin -d /home/user1 -s /bin/bash user1`: Crear un nuevo usuario perteneciente al grupo "admin".
5. `userdel user1`: crear un nuevo usuario.
6. `userdel -r user1`: borrar un usuario ("r" elimina el directorio Home).
7. `usermod -c "User EIP" -g /usr -d /tmp user1 -s /bin/bash user1`: cambiar los atributos del usuario.
8. `passwd`: cambiar contraseña.
9. `passwd user1`: cambiar la contraseña de un usuario (solo para root).
10. `chage -E 2011-12-31 user1`: colocar un plazo para la contraseña del usuario. En este caso dice que la clave expira el 31 de diciembre de 2011.
11. `pwdck`: chequear la sintaxis correcta el formato de fichero de `/etc/passwd` y la existencia de usuarios.
12. `grpck`: chequear la sintaxis correcta y el formato del fichero `/etc/group` y la existencia de grupos.
13. `newgrp grupo_nombre`: registra a un nuevo grupo para cambiar el grupo predeterminado de los ficheros creados recientemente.

Permisos en Ficheros (Usa "+" para colocar permisos y "-" para eliminar)

1. `ls -ls`: Mostrar permisos.
2. `ls -lsp | pr -ts -w60COLUMNS`: Mostrar la terminal en 3 columnas.
3. `chmod ugo=rwx directory1`: otorgar permisos de lectura (r), escritura (w) y ejecución (x) al propietario (u), al grupo (g) y a otros (o) sobre el directorio "directory1".
4. `chmod go=rwx directory1`: quitar permisos de lectura (r), escritura (w) y (x) al grupo (g) y otros (o) sobre el directorio "directory1".
5. `chmod user1 file1`: cambiar el dueño de un fichero.

6. `chown -R user1:directory1`: cambiar el propietario de un directorio y de todos los ficheros y directorios contenidos dentro.
7. `chgrp group1 file1`: cambiar grupo de ficheros.
8. `chown user1:group1 file1`: cambiar usuario y el grupo propietario de un fichero.
9. `find / -perm -u+s`: visualizar todos los ficheros del sistema con SUID configurado.
10. `chmod u+s binfile1`: colocar el bit SUID en un fichero binario. El usuario que accediendo ese fichero adquiere los mismos privilegios como dueño.
11. `chmod u-s binfile1`: deshabilitar el bit SUID en un fichero binario.
12. `chmod g+s /home/public`: colocar un bit SGID en un directorio –similar al SUID pero por directorio.
13. `chmod g-s /home/public`: deshabilitar un bit SGID en un directorio.
14. `chmod o+s /home/public`: colocar un bit STICKY en un directorio. Permite el borrado de ficheros solamente a los dueños legítimos.
15. `chmod o-s /home/public`: deshabilitar un bit STICKY en un directorio.

Atributos especiales en ficheros (Usa "+" para colocar permisos y "-" para eliminar)

1. `chattr +a file1`: permite escribir abriendo un fichero solamente modo append.
2. `chattr +c file1`: permite que un fichero sea comprimido / descomprimido automáticamente.
3. `chattr +d file1`: asegura que el programa ignore borros los ficheros durante la copia de seguridad.
4. `chattr +i file1`: convierte el fichero en invariable, por lo que no puede ser eliminado, alterado, renombrado, ni enlazado.
5. `chattr +s file1`: permite que un fichero sea borrado de forma segura.
6. `chattr +S file1`: asegura que un fichero sea modificado. Los cambios son escritos en modo synchronous (con sync).
7. `chattr +u file1`: le permite recuperar el contenido de un fichero aun si este está corrompido.
8. `lsattr`: mostrar atributos especiales.

Archivos y Ficheros comprimidos

1. `unzip file1.tar`: descomprime un fichero llamado file1.tar.
2. `bzip2 file1`: comprime un fichero llamado file1.
3. `gunzip file1.gz`: descomprime un fichero llamado file1.gz.
4. `gzip file1`: comprime un fichero llamado file1.
5. `gzip -9 file1`: comprime con compresión máxima.
6. `rar a file1.rar var_1file`: crear un fichero rar llamado file1.rar.
7. `rar a file1.rar file1 file2 dir1`: comprimir file1, file2 y dir1 simultáneamente.
8. `rar x file1.rar`: descomprimir archivo rar.
9. `unrar x file1.rar`: descomprime archivo rar.
10. `tar -xvf archive.tar`: crear un tarball descomprimido.
11. `tar -xvf archive.tar file1 file2 dir1`: crear un archivo (contenido file1, file2 y dir1).
12. `tar -tf archive.tar`: mostrar los contenidos de un archivo.
13. `tar -xvf archive.tar`: extraer un tarball.
14. `tar -xvf archive.tar -C /tmp`: extraer un tarball en /tmp.
15. `tar -cvf archive.tar file1 file2`: crear un tarball comprimido dentro de bzip2.
16. `tar -xvf archive.tar file1`: descomprimir un archivo tar comprimido en bzip2.
17. `tar -cvf archive.tar file1`: crear un tarball comprimido en gzip.
18. `tar -xvf archive.tar file1`: descomprimir un archivo tar comprimido en gzip.
19. `zip file1.zip file1`: crear un archivo comprimido en zip.
20. `zip -r file1.zip file1 file2 dir1`: comprimir, en zip, varios archivos y directorios de forma simultánea.
21. `unzip file1.zip`: descomprimir un archivo zip.

Paquetes RPM (Red Hat, Fedora y similares)

1. `rpm -vih package.rpm`: instalar un paquete rpm.
2. `rpm -ivh --nodeps package.rpm`: instalar un paquete rpm ignorando las peticiones de dependencias.
3. `rpm -U package.rpm`: actualizar un paquete rpm sin cambiar la configuración de los ficheros.
4. `rpm -F package.rpm`: actualizar un paquete rpm solamente si este está instalado.
5. `rpm -e package_name.rpm`: eliminar un paquete rpm.
6. `rpm -qa`: mostrar todos los paquetes rpm instalados en el sistema.
7. `rpm -qa | grep httpd`: mostrar todos los paquetes rpm con el nombre "httpd".
8. `rpm -qi package_name`: obtener información en un paquete específico instalado.
9. `rpm -qf "Systemd EnvironmentdDaemon"`: mostrar los paquetes rpm de un grupo software.
10. `rpm -ql package_name`: mostrar lista de ficheros dados por un paquete rpm instalado.
11. `rpm -qr package_name`: mostrar lista de configuración de ficheros dados por un paquete rpm instalado.
12. `rpm -q package_name --whatrequires`: mostrar lista de dependencias solicitada para un paquete rpm.
13. `rpm -q package_name --whatprovides`: mostrar la capacidad dada por un paquete rpm.
14. `rpm -q package_name --scripts`: mostrar los scripts ejecutables durante la instalación y eliminación.
15. `rpm -q package_name --changelog`: mostrar el historial de cambios de un paquete rpm.

16. `rpm -qf /archivos/distribuid.com`: verificar cuál paquete rpm pertenece a un fichero dado.
17. `rpm -qp package.rpm`: mostrar lista de ficheros dados por un paquete rpm que aún no ha sido instalado.
18. `rpm --import /media/extra.com/RPM-GPG-KEY`: importar la firma digital de la llave pública.
19. `rpm --checksig package.rpm`: verificar la integridad de un paquete rpm.
20. `rpm -qa rpm-pubkey`: verificar la integridad de todos los paquetes rpm instalados.
21. `rpm -X package_name`: chequear el tamaño del fichero, licencias, tipos, dueño, grupo, chequeo de checksum de MD5 y última modificación.
22. `rpm -Va`: chequear todos los paquetes rpm instalados en el sistema. Usar con cuidado.
23. `rpm -Vp package.rpm`: verificar un paquete rpm no instalado todavía.
24. `rpm2cpio package.rpm | cpio --extract --make-directories /dev/`: extraer fichero ejecutable desde un paquete rpm.
25. `rpm -kch /var/extra/extra/OS/MSI/arch/package.rpm`: instalar un paquete coninado desde una fuente rpm.
26. `rpm2cpio --extract package_name.rpm`: convertir un paquete rpm desde una fuente rpm.

Actualizador de paquetes YUM (Red Hat, Fedora y similares)

1. `yum install package_name`: descargar e instalar un paquete rpm.
2. `yum localinstall package_name.rpm`: más instalar un RPM y tratará de resolver todas las dependencias para él, usando los repositorios.
3. `yum update package_name.rpm`: actualizar todos los paquetes rpm instalados en el sistema.
4. `yum update package_name`: actualizar / actualizar un paquete rpm.
5. `yum remove package_name`: eliminar un paquete rpm.
6. `yum list`: lista / todos los paquetes instalados en el sistema.
7. `yum search package_name`: Encontrar un paquete en repositorio rpm.
8. `yum clean packages`: limpiar los caché rpm borrando los paquetes descargados.
9. `yum clean headers`: eliminar todos los ficheros de encabezamiento que el sistema usa para manejar la dependencia.
10. `yum clean all`: eliminar desde los paquetes caché y ficheros de encabezado.

Paquetes Deb (Debian, Ubuntu y derivados)

1. `dpkg -i package.deb`: instalar / actualizar un paquete deb.
2. `dpkg -r package_name`: eliminar un paquete deb del sistema.
3. `dpkg -l`: mostrar todos los paquetes deb instalados en el sistema.
4. `dpkg -l | grep httpd`: mostrar todos los paquetes deb con el nombre "httpd".
5. `dpkg -f package_name`: obtener información de un paquete específico instalado en el sistema.
6. `dpkg -l package_name`: mostrar lista de ficheros dados por un paquete instalado en el sistema.
7. `dpkg --get-selections package.deb`: mostrar lista de ficheros dados por un paquete no instalado todavía.
8. `dpkg -f /dev/null`: verificar cuál paquete pertenece a un fichero dado.

Actualizador de paquetes APT (Debian, Ubuntu y derivados)

1. `apt-get install package_name`: instalar / actualizar un paquete deb.
2. `apt-get install package_name`: instalar / actualizar un paquete deb desde un cdrom.
3. `apt-get update`: actualizar la lista de paquetes.
4. `apt-get upgrade`: actualizar todos los paquetes instalados.
5. `apt-get remove package_name`: eliminar un paquete deb del sistema.
6. `apt-get check`: verificar la correcta instalación de las dependencias.
7. `apt-get clean`: limpiar caché desde los paquetes descargados.
8. `apt-cache search keyword-package`: mostrar lista de paquetes que corresponden a la serie o palabras buscadas.

Ver el contenido de un fichero

1. `cat file`: ver los contenidos de un fichero comenzando desde la primera línea.
2. `tac file`: ver los contenidos de un fichero comenzando desde la última línea.
3. `more file`: ver el contenido a lo largo de un fichero.
4. `less file`: parecido al comando "more" pero permite salvar el movimiento en el fichero así como el movimiento hacia atrás.
5. `head -3 file`: ver las dos primeras líneas de un fichero.
6. `tail -2 file`: ver las dos últimas líneas de un fichero.
7. `tail -f /var/log/messages`: ver en tiempo real qué ha sido añadido al fichero.

Manipulación de texto

1. `cat file1 file2 ... |> concatenated <- file1 | cat file2 | cat file3`: utilidad general para la manipulación de texto mediante PIPE, STDIN y STDOUT.
2. `cat file1 |> command | cat, grep, mv, cp, mv, etc...> result.cat`: utilidad general para manipular un texto de un fichero y escribir el resultado en un fichero nuevo.

1. `cat file1 | command sed, grep, awk, grep, etc. > result.txt`: simple general para manipular un texto de un fichero y añadir resultado en un fichero existente.
2. `grep Aug /var/log/messages`: buscar palabras "Aug" en el fichero "/var/log/messages".
3. `grep ^Aug /var/log/messages`: buscar palabras que comiencen con "Aug" en el fichero "/var/log/messages".
4. `grep [0-9] /var/log/messages`: seleccionar todas las líneas del fichero "/var/log/messages" que contienen números.
5. `grep Aug -R /var/log/*`: buscar la cadena "Aug" en el directorio "/var/log" y debajo.
6. `sed -i s/strings/strings2/g example.txt`: reemplazar "strings" con "strings2" en ejemplo.txt
7. `sed 's/.*' example.txt`: eliminar todas las líneas en blanco desde el ejemplo.txt
8. `sed 's/.*' /s/.*' example.txt`: eliminar comentarios y líneas en blanco de ejemplo.txt.
9. `echo "example" | tr '[:lower:]' '[:upper:]'`: convierte minúsculas en mayúsculas.
10. `sed -e 1d result.txt`: elimina la primera línea del fichero ejemplo.txt.
11. `sed -n /strings/p`: visualizar solamente las líneas que contienen la palabra "strings".

Establecer caracter y conversión de ficheros

1. `dos2unix fileunix.txt fileunix.txt`: convertir un formato de fichero text desde MS-DOS a UNIX.
2. `unix2dos fileunix.txt fileunix.txt`: convertir un formato de fichero de texto desde UNIX a MS-DOS.
3. `recode -l HTML < page.txt > page.html`: converte un fichero de texto en html.
4. `recode -l | more`: mostrar todas las conversiones de formato disponibles.

Análisis del sistema de ficheros

1. `badblocks -v /dev/hda1`: Chequea los bloques defectuosos en el disco hda1.
2. `fsck /dev/hda1`: reparar / chequear la integridad del fichero del sistema Linux en el disco hda1.
3. `fsck.ext2 /dev/hda1`: reparar / chequear la integridad del fichero del sistema ext 2 en el disco hda1.
4. `fsckfs /dev/hda1`: reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
5. `fsckfs -j /dev/hda1`: reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
6. `fsck.ext3 /dev/hda1`: reparar / chequear la integridad del fichero del sistema ext 3 en el disco hda1.
7. `fsck.vfat /dev/hda1`: reparar / chequear la integridad del fichero fat32 en el disco hda1.
8. `fsck.msdos /dev/hda1`: reparar / chequear la integridad de un fichero del sistema dos en el disco hda1.
9. `badblocks /dev/hda1`: reparar / chequear la integridad de un fichero del sistema dos en el disco hda1.

Formatear un sistema de ficheros

1. `mkfs /dev/hda1`: crear un fichero de sistema tipo Linux en la partición hda1.
2. `mkfs2k /dev/hda1`: crear un fichero de sistema tipo Linux ext 2 en hda1.
3. `mkfs2k -j /dev/hda1`: crear un fichero de sistema tipo Linux ext3 (particionado) en la partición hda1.
4. `mkfs -e vfat 32-1 /dev/hda1`: crear un fichero de sistema FAT32 en hda1.
5. `fdformat -a /dev/hda1`: formatear un disco floppy.
6. `mkswap /dev/hda1`: crear un fichero de sistema swap.

Trabajo con la SWAP

1. `mkswap /dev/hda3`: crear fichero de sistema swap.
2. `swapon /dev/hda3`: activando una nueva partición swap.
3. `swapon /dev/hda2, /dev/hda3`: activar dos particiones swap.

Salvas (Backup)

1. `dump -0f /tmp/home0.bak home`: hacer una salva completa del directorio "/home".
2. `dump -1f /tmp/home0.bak home`: hacer una salva incremental del directorio "/home".
3. `restore -f /tmp/home0.bak`: restaurando una salva incrementalmente.
4. `rsync -avgv -delete home /tmp`: sincronización entre directorios.
5. `rsync -avgv -e ssh -delete home ip_addr:/tmp`: rsync a través del títul SSH.
6. `rsync -ax-e ssh -delete ip_addr/home/public /home/local`: sincronizar un directorio local con un directorio remoto a través de ssh y de compresión.
7. `rsync -ax-e ssh -delete /home/local ip_addr/home/public`: sincronizar un directorio remoto con un directorio local a través de ssh y de compresión.
8. `dd bs=1M if=/dev/hda1 | gzip | ssh user@ip_addr 'dd of=/dev/gp'`: hacer una salva de un disco duro en un otro remoto a través de ssh.
9. `dd if=/dev/sda of=/tmp/gp.gz`: salvar el contenido de un disco duro a un fichero. (En este caso el disco duro es "sda" y el fichero "file").
10. `tar -Juf backup.tar /home/user`: hacer una salva incremental del directorio "/home/user".
11. `(cd /tmp/local && tar c .) | ssh -C user@ip_addr '(cd /home/home && tar x -p)'`: copiar el contenido de un directorio en un directorio remoto a través de ssh.
12. `(tar c /home) | ssh -C user@ip_addr '(cd /home/backup-home && tar x -p)'`: copiar un directorio local en un directorio remoto a través de ssh.
13. `tar cf- . | (cd /tmp/backup ; tar xf-)`: copia local conservando las licencias y enlaces desde un directorio a otro.

14. `find /home/user1 -name "*.tar" | xargs cp -av -target-directory=/home/backups/ -parents` Encontrar y copiar todos los ficheros con extensión ".tar" de un directorio a otro.
15. `find /var/log -name "*.log" | tar cv -files-from=- | bzip2 > log.tar.bz2` encontrar todos los ficheros con extensión ".log" y hacer un archivo bzip
16. `dd if=/dev/tda of=/dev/hd3 bs=512 count=1` hacer una copia del MBR (Master Boot Record) a un disco floppy.
17. `dd if=/dev/hd3 of=/dev/hda bs=512 count=1` restaurar la copia del MBR (Master Boot Record) salvada en un floppy.

CD-ROM

1. `cdrdao -v -i /dev/cdrom -o /dev/cdrom -f /dev/cdrom` Empezar o borrar un cd registrable.
2. `mksdisc /dev/cdrom > cd.iso` crear una imagen iso de cdrom en disco.
3. `mksdisc /dev/cdrom | gzip > cd.img.gz` crear una imagen comprimida iso de cdrom en disco.
4. `mksdisc -j -allow-loading-data -t -v "data1 ISO" -lsc data1 && -o /cd iso data_01` crear una imagen iso de un cdrom iso.
5. `cdrdao -v -i /dev/cdrom -o /dev/cdrom` quemar una imagen iso.
6. `gzip -dc cd.img.gz | cdrdao /dev/cdrom -` quemar una imagen iso comprimida.
7. `mount -o loop cd.iso /mnt/iso` montar una imagen iso.
8. `cd-paranoia -B` llevar copias de un cd a ficheros wav.
9. `cd-paranoia -T30` llevar las 3 primeras canciones de un cd a ficheros wav.
10. `cdrdao -scanbus` escanear bus para identificar el canal iso.
11. `dd if=/dev/hdr | md5sum` hacer funcionar md5sum en un dispositivo, como un CD.

Trabajo con la RED (LAN y Wi-Fi)

1. `ifconfig eth0` mostrar la configuración de una tarjeta de red Ethernet.
2. `ifup eth0` activar una interfaz "eth0".
3. `ifdown eth0` desactivar una interfaz "eth0".
4. `ifconfig eth0 192.168.1.1 netmask 255.255.255.0` configurar una dirección IP.
5. `ifconfig eth0 promisc`, configurar "eth0"en modo catch para obtener los paquetes (sniffing)
6. `ifconfig eth0` activar la interfaz "eth0" en modo dhcp.
7. `route -n` mostrar mesa de enrutado.
8. `route add -net 0.0.0.0 gw IP_Gateway` configurar entrada predeterminada.
9. `route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1` configurar ruta estática para buscar la red 192.168.0.0/16.
10. `route del 0.0.0.0 gw IP_gateway` eliminar la ruta estática.
11. `echo "1" > /proc/sys/net/ipv4/ip_forward` activar el enrutado ip.
12. `hostname`: mostrar el nombre del host del sistema.
13. `host www.example.com`: buscar el nombre del host para resolver el nombre a una dirección (ip(1)).
14. `nslookup www.example.com`: buscar el nombre del host para resolver el nombre a una dirección ip y un reverse(2).
15. `ip link show` mostrar el estado de enlace de todas las interfaces.
16. `mii-tool eth0`: mostrar el estado de enlace de "eth0".
17. `ethtool eth0`: mostrar las estadísticas de tarjeta de red "eth0".
18. `netstat -tup`: mostrar todas las conexiones de red activas y sus PID.
19. `netstat -tupl`: mostrar todos los servicios de escucha de red en el sistema y sus PID.
20. `tcpdump tcp port 80` mostrar todo el tráfico HTTP.
21. `brctl scan`: mostrar las redes inalámbricas.
22. `wepconfig eth0`: mostrar la configuración de una tarjeta de red inalámbrica.
23. `whois www.example.com`: buscar en base de datos Whois.

Redes de Microsoft Windows (SAMBA)

1. `nblookup ip_addr`: resolución de nombre de red bios.
2. `nmlookup <ip_addr`: resolución de nombre de red bios.
3. `smbclient -L ip_addr/hostname`: mostrar los datos remotos de un host en windows.

Tablas IP (CORTAFUEGOS)

1. `iptables -f /etc -L`: mostrar todas las cadenas de la tabla de filtro.
2. `iptables -f nat -L`: mostrar todas las cadenas de la tabla nat.
3. `iptables -f filter -F`: borrar todas las reglas de la tabla de filtro.
4. `iptables -f nat -F`: borrar todas las reglas de la tabla nat.
5. `iptables -f filter -X`: borrar cualquier cadena creada por el usuario.
6. `iptables -f filter -A INPUT -p tcp -d port1 -j ACCEPT`: permitir las conexiones telnet para "port1".
7. `iptables -f filter -A OUTPUT -p tcp -s port1 -j DROP`: bloquear las conexiones HTTP para "port1".
8. `iptables -f filter -A FORWARD -p tcp -d port1 -j ACCEPT`: permitir las conexiones POP a una cadena "destino".
9. `iptables -f filter -A INPUT -j LOG --log-prefix "DROP INPUT"`: registrando una cadena de entrada.

10. `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`: configurar un NAT (Puerto de traducción de dirección) en `eth0`, enviando los paquetes de salida formados.
11. `iptables -t nat -A PREROUTING -d 192.168.0.1 -p tcp -m tcp --dport 22 -j DNAT --to-destination 10.0.0.2:22`: redirigir los paquetes dirigidos de `192.168.0.1` a `10.0.0.2`.

Monitoreando y depurando

1. `top`: mostrar las tareas de Linux usando la proporción CPU.
2. `ps -efw`: muestra las tareas Linux.
3. `ps -e -u pid,args -Sort=`: muestra las tareas Linux en un modo jerárquico.
4. `psaux`: mostrar un árbol (árbol de procesos).
5. `kill -9 ID_Proceso`: forzar el cierre de un proceso y terminar.
6. `kill -1 ID_Proceso`: forzar un proceso para recargar la configuración.
7. `lsof -p PID`: mostrar una lista de ficheros abiertos por proceso.
8. `lsof /ruta/fuero/`: muestra una lista de ficheros abiertos en un directorio del sistema.
9. `strace -e la-sistema`: mostrar las llamadas del sistema hechas y recibidas por un proceso.
10. `strace -f -e open la-sistema`: mostrar las llamadas a la biblioteca.
11. `watch -n1 'cat /proc/interrupts'`: mostrar interrupciones en tiempo real.
12. `cat /proc`: mostrar historial de proceso.
13. `lsmod`: mostrar el kernel cargado.
14. `free -m`: muestra el estado de la RAM en megabytes.
15. `smartctl -A /dev/sda`: monitorizar la fiabilidad de un disco duro a través de SMART.
16. `smartctl -t /dev/sda`: chequear si SMART está activado en un disco duro.
17. `cat /var/log/dmccmp`: mostrar eventos inherentes al proceso de carga del kernel.
18. `cat /var/log/messages`: mostrar los eventos del sistema.

Otros comandos útiles

1. `apropos keyword`: mostrar una lista de comandos que pertenecen a las palabras claves de un programa. Son útiles cuando no sabes qué hace tu programa, pero de vez en cuando el nombre del comando.
2. `man ping`: mostrar las páginas del manual en línea; por ejemplo, en un comando `ping`, usar la opción `hal` para encontrar cualquier comando relacionado.
3. `whatis keyword`: muestra la descripción de lo que hace el programa.
4. `mkisofs -b/dev/sda "name-r"`: crear un floppy bootable.
5. `gpg -c file`: codificar un fichero con guardia de seguridad GPG.
6. `gpg file.gpg`: decodificar un fichero con guardia de seguridad GPG.
7. `wget -c www.example.com`: descargar un sitio web completo.
8. `wget -c www.example.com/files`: descargar un fichero con la posibilidad de parar la descarga y reanudar más tarde.
9. `echo wget -c www.example.com/files.txt | at 0900`: programar una descarga a cualquier hora. En este caso, empezaría a las 9 horas.
10. `lsd /usr/bin/ls`: mostrar las librerías compartidas requeridas por el programa `ls`.
11. `alias [he/hist]`: crear un alias para un comando -he= historial.
12. `chsh`: cambiar el comando Shell.
13. `chsh -hal-shell`: es un comando adecuado para saber si tienes que hacer cambios en una terminal.
14. `who-a`: mostrar quien está registrado, e imprimir para del último sistema de impresión, procesos muertos, procesos de registro de sistema, procesos activos producidos por `mail`, funcionamiento actual y últimos cambios del reloj del sistema.

Fuente: <http://git.io/venclub.es/>

Facebook Twitter GitHub YouTube

What's Related?



Opciones de contraseñas de Gmail, Yahoo



Hackers & Developers en Kevlar de Softw



SQL Injection Cheat Sheet



Estructura Interna de los ficheros



Recopilación de PDFs sobre Seguridad



Author & Editor